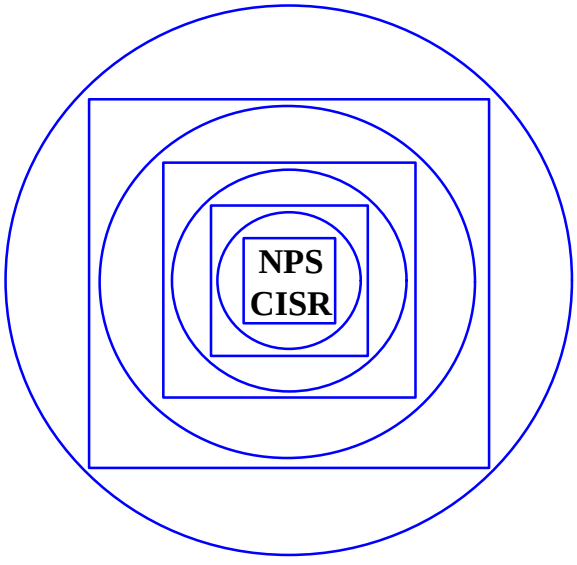
Naval Postgraduate School

Center for Information Systems Security Studies and Research

NPS CISR

Annual Report
July 1998



Naval Postgraduate School

Center for Information Systems Security Studies and Research

NPS CISR

Annual Report
July 1998

By
Cynthia E. Irvine

Naval Postgraduate School
Department of Computer Science
Code CS/Ic Monterey, California 93943-5118
(831) 656-2461
Email: irvine@cs.nps.navy.mil

A report developed as a guide to work carried out over the last year by the NPS CISR Research Group and the Computer Security Laboratory

http://cisr.nps.navy.mil/

Executive Summary

Established in October 1996, the Naval Postgraduate School Center for Information Systems Security (INFOSEC) Studies and Research (NPS CISR) is dedicated to the development of instructional materials and courses for graduate-level education in computer security and to the pursuit of research on a variety of INFOSEC topics.

This report summarizes the accomplishments of NPS CISR over the past year and focuses on the eight primary areas in which NPS CISR serves the needs of DoD/DoN.

- Curriculum Development ensures that a coherent and comprehensive program in INFOSEC foundations and technology is presented at the university and postgraduate levels. Current enrollments are over 290 students annually.
- Development of the Computer Security Laboratory supports the INFOSEC teaching and research programs at NPS and permits experimentation with evolving technology. The Laboratory is used extensively for classes and thesis research.
- Faculty Development fosters the insertion of INFOSEC concepts at appropriate points in general computer science courses and involves interested faculty members in leading-edge INFOSEC research problems.
- A Visiting Professor program brings INFOSEC experts to NPS to enhance courses and conduct collaborative research with faculty and students.
- An Invited Lecture Series injects commercial and military relevance into the NPS CISR courses and research.
- An Academic Outreach program permits other, non-CISR academic institutes to benefit from the INFOSEC education and research developments at NPS.Through workshops, the Internet, and emerging technologies NPS CISR shares its expertise in systems security education.
- Graduate Utilization ensures that NPS graduates involved in NPS CISR courses and research are recognized so that their expertise can be applied to the wide variety of INFOSEC challenges in DoD and U.S. Government.
- Research ensures that NPS CISR programs are at the leading edge of computer and network security developments. Topics of importance to DoD/DoN are explored.

A major by-product of this effort is high-quality research focusing on important INFOSEC problems, bringing together the appropriate resources to solve those problems, and serving DoN, DoD, and U.S. Government needs.

1. Introduction

The Naval Postgraduate School is fortunate to be the home to what many researchers in the computer and network security community consider to be the preeminent program in the United States combining research and studies in information systems security (INFOSEC) and information assurance (IA). Since its inception, the Naval Postgraduate School Center for Information Systems Security Studies and Research (NPS CISR) has fostered an environment in which faculty, staff, and students work together to understand the information assurance requirements of DoD and to address the challenges presented by those requirements through careful analysis and research.

The need for focussed effort in information security and assurance is evident. The development of military strategy and tactics for warfare in the information age is of growing importance and has, as its principal objective, information superiority for U.S. forces engaged in battle on land, at sea or in the air. A key aspect of achieving information superiority is the protection of critical national information assets. Increasingly, military systems are dependent upon the national infrastructure for critical services.Today the United States faces an enormous problem. All aspects of the national infrastructure, from telecommunications to health care and from air traffic control to power systems, depend upon the correct operation of computers and networks. The security of those networks is crucial to the health of that infrastructure, yet security is often ignored as a fundamental requirement. Providing adequate protection for these information assets is a concern for the U.S. military and presents many new scientific and technical challenges in the area of INFOSEC and IA.

The October 1997 report of the Presidential Commission on Critical Infrastructure Protection (PCCIP) recommends *"education on methods of reducing vulnerabilities and responding to attacks on critical infrastructures", "programs for curriculum development at the undergraduate and graduate levels in resilient system design practices,"* and efforts to make the *"required skill set much broader and deeper in educational level [for] computer scientists, network engineers, electronics engineers, [and] business process engineers."*

Anticipating these recommendations by more than five years, the Naval Postgraduate School, with support from the National Security Agency (NSA), initiated a modest effort within the Computer Science Department to build a prototype program with three objectives: the development of courses on computer and network security based in a strong curriculum of science and engineering; research in information system security; and development of a cadre of officer-graduates with a thorough understanding of computer and network security issues. An essential notion behind the development of NPS CISR is that the security of information systems must be founded on scientific and engineering principles which are used to construct secure systems rather than to discover after deployment that systems are inadequate. (A situation that is woefully frequent today.)

Within a few years, the success of these early efforts was clear. Hundreds of students were attending our flag-ship course and there was considerable interest in research. In response, an expansion of the program began and in the fall of 1994 the NPS Academic Council approved the addition of a sequence of new courses to the Computer Science curriculum. Combined with the Naval Postgraduate School thesis requirement for all Masters-level students, the academic program provides graduates with the knowl-

edge needed to manage and contribute to engineering teams tasked not only to design and build secure systems, but also to configure and maintain them.The strong science and engineering education of NPS CISR graduates helps them to address new problems and to distinguish "snake oil" and marketing hyperbole from credible security solutions.

Today, NPS CISR involves the research of thirteen faculty and staff members, thesis students from several departments, and classes with total enrollments of approximately 290 students annually.

2. Status of NPS CISR Programs

This section is intended to provide the current status of NPS CISR programs.

2.1 Curriculum Development

Through courses development, NPS CISR is working toward a comprehensive, relevant INFOSEC speciality track that uses and is integrated with the computer science curriculum and that reflects broad perspectives on security problems.

Figure 1. Annually, hundreds of students are enrolled in NPS CISR courses. Each class is limited to 25 students. Here Prof. Warren, center front, poses with some of his students in the Computer Security Laboratory.

The INFOSEC track benefits students in the following ways:

- It serves both beginning and advanced students,
- It provides courses accessible by students school-wide,
- It provides students with a strong foundation upon which to base advanced course work in computer and INFOSEC,
- It involves students in ongoing research and technology development efforts associated with computer security and INFOSEC, and
- It enhances students' laboratory experience through the hands-on use of secure systems.

Students receive a graduate degree in computer science with an area of specialization in INFOSEC.

Each course at NPS is only twelve weeks long, and care is taken to integrate the courses into a coherent sequence. The INFOSEC program avoids compartmentalization within courses, and presents students with principles and techniques, such as formal methods and good management practice, that span multiple aspects of computer security. Emphasis is placed on the fundamental principles underlying the development of computer systems designed to enforce critical security policies. This strong foundation prepares students to address research and operational problems in INFOSEC. Using case studies, students understand how past problems have been solved and have an opportunity to consider current topics. Issues associated with incremental approaches to security associated with risk management are discussed.

In FY98 NPS CISR offered the full complement of courses planned for the program. These included

- Introduction to Computer Security
- Secure Management of Systems
- Network Security
- Secure Systems
- Database Security
- Security Policies, Models and Formal Methods
- Advanced Topics in Computer Security

New courses in FY98 included Secure System and Database Security. Other courses that were taught for the second time in FY98 are Secure Management of Systems, Network Security and Security Policies, Models and Formal Methods.

Secure Systems combined both lecture and laboratory activities to give students an understanding of the principles and design issues involved in constructing systems to enforce security policies. Laboratory activity allowed students to consider low-level hardware issues.

Database Security begins with an examination of policies and system architectures for secure database management systems. Students then designed a secure database implementation based upon a published system architecture and developed a small demonstration prototype.

In the previous year we restructured our flagship course, Introduction to Computer Security, so that it is available to second and third quarter students. The benefits of this change are being realized as students carry forward an appreciation of critical INFOSEC issues to their subsequent classes. Students interested in computer security can plan their course of study to include additional INFOSEC courses. Those wishing to pursue thesis research have longer to work with faculty and sponsors, both to select track electives and design thesis research.

We have found that the use of laboratory material as well as demonstration given as part of the class have helped to reinforce concepts presented during lectures. With real examples, students have a much firmer grip on the benefits of what is often viewed as an intangible system property, i.e. that the system enforces security policy correctly.

At the request of the US Air Force Academy, NPS CISR developed a one-year fast-track Masters degree program for selected Academy Computer Science graduates. The officers entering this program move directly into graduate-level work, by-passing the first year of the typical NPS program. The program is possible for two reasons. First, the student comes to NPS directly from a strong undergraduate program and requires no reintroduction to academics and no exposure to undergraduate computer science concepts. Second, this accelerated computer science curriculum requires four quarters, twelve courses and four thesis “slots.” The qualifications of the students combined with the density and intensity of the program makes the one-year Master of Science degree program feasible.

2.2 Computer Security Laboratory

The ultimate objective of INFOSEC studies is to improve security in real systems. Thus, practical laboratory experience is crucial for an effective INFOSEC program. Laboratory exercises in the form of tutorials and projects help to reinforce and extend concepts conveyed in lectures as well as help prepare students for effective thesis research. Laboratory facilities can provide a test-bed for initiating promising faculty and student research on current INFOSEC problems.

With class enrollments of approximately 290 students in FY98, the Computer Security Laboratory has been heavily utilized. It is

also the site of a considerable portion of the thesis research being conducted by NPS CISR students. As shown in Figure 2, the laboratory can be quite busy.

Figure 2. The Computer Security Laboratory is used both to support classes and for thesis research. In the foreground, CPT Wright works with David Shifflett on thesis research, while a class works on a laboratory exercises in the background

Laboratory improvements over the past year have included:

- Acquisition of an ATM switch and test network for research on security of IP over ATM networks
- Development of an IT-21 compliant network consisting of a Windows NT Server and four Windows NT client workstations. These have been used for COTS-based security experiments, classes, and research.
- Upgrades of two Wang XTS 300 systems to the latest software version. This software upgrade resulted in shipment of two new XTS 300 platforms from the vendor. The old platforms have been reconfigured to run other software and are available for student use.
- Acquisition of an SGI O2 for use as a web server. The server is configured with only two user accounts: the administrator and the webmaster. Security patches are installed and software to monitor suspicious activity is in place. The server has been the site of a considerable number of failed probes.
- A laptop-based demonstration system for use in the classroom, tutorials, lectures, and workshops. The equipment includes a portable projector and a laptop.
- A 23 Gb hard drive used for digitization of video tapes for the production of web-based instructional materials.
- A microphone for use with the professional video camera used to record invited lectures and other events. The camera is loaned on an as-needed basis to NPS CISR by the computer graphics curriculum.
- Research and course development platforms for NPS CISR faculty and staff.
- A variety of software components. A few examples are:
  - CD creation software
  - voice activated editing tools
  - disk partitioning and boot selection software
  - CDSA from Intel and RSA
  - TIS Gauntlet - on loan from sponsors of a thesis research project

Most NPS CISR courses include a lab component. As existing courses are refined and new ones developed, corresponding lab exercises are prepared or updated. An objective of the NPS CISR program is to allow students to understand the kinds of technologies that are available to solve current computer security problems and to consider

potential future technologies. Students are given first-hand experience in using a variety of trusted systems and explore topics in security policy enforcement, security technology for database systems, monolithic and networked trusted computing techniques, and tools to support the development of trusted systems.

Support from sponsors has sustained our ability to have a full time laboratory manager/systems programer to assist with the operation of the computer security laboratory. His participation in supporting both classes and student research has been invaluable. Classes he has supported include: Introduction to Computer Security; Secure Management of Systems; Secure Systems; Database Security; Network Security; and Security Policies, Models, and Formal Methods. The many software and hardware upgrades to the laboratory constituted another aspect of his support activities.

Our laboratory manager has also provided students with laboratory support for their thesis work. This includes ensuring the proper operation of our primary high assurance platforms, the XTS 300 systems, PCs, and Unix systems. In order to conduct research on the security aspects of remote execution, several specialized applications are supported. In many cases, support of these advanced programming and execution environments required reconfiguration and with frequent updates and careful management. Maintenance contracts for the high assurance systems ensures access to updates as the systems evolve.

During the past year, NPS CISR has been able to hire an assistant whose duties include work in the laboratory. These include

- The development of web pages supporting NPS CISR activities such as: courses, the invited lecture series, research and academic outreach,
- The production of CDs containing course and invited lecture materials,
- Cataloging, creating backups for, digitization and editing of video materials from the invited lecture series, and
- Support of workshops conducted by NPS CISR.

2.3 Faculty Development

The Computer Science Department at NPS has a group of permanent faculty members whose expertise can be applied immediately to current computer security research challenges. These individuals are either directly engaged in computer security research or are engaged in research which is transferable and highly relevant to critical problems in computer security.

NPS CISR helps to stimulate INFOSEC research by building upon the expertise selected faculty members have demonstrated in other areas. These individuals are asked to apply their expertise to current INFOSEC problems. Benefits of this aspect of the program include:

- A deepening of NPS faculty appreciation of INFOSEC problems and issues,
- Increasing the number of faculty able to support NPS CISR,
- Productive new INFOSEC research approaches, and
- Further student participation through the supervision of a larger cadre of qualified faculty members.

Professor Geoff Xie received support through NPS CISR to conduct research on security techniques for Asynchronous Transfer Mode (ATM) networks. Challenges to the security of ATM involve the bindings of the tags associated with virtual channels to the IP packets assigned to them. With two thesis students, Dr. Xie is exploring proto-

cols to enhance IP/ATM security.

Professor Bert Lundy's area of expertise is formal modeling of low-level network protocols. As security must be a consideration in protocol design and analysis, his participation with the faculty development program contributes to the incorporation of security at fundamental levels in networks.

2.4 Visiting Professor Program

The Visiting Professor Program is intended to strengthen and expand the INFOSEC research and education program at NPS and to accelerate technology transfer between academe and industry. The program facilitates the development of INFOSEC curricula by obtaining access to experienced contributors in the field of computer science and INFOSEC.

Individuals selected to fill the visiting professor chair in INFOSEC at NPS CISR must be acknowledged experts in the field of computer security or a field closely aligned with computer security objectives. Visiting professors assist NPS faculty with the development of INFOSEC courses for the new specialty track. These professors teach computer science classes, conduct basic research, assist students with thesis work, and serve as mentors for faculty members interested in becoming involved in INFOSEC.

In May 1998 Dr. James Bret Michael joined NPS CISR as a visiting associate Professor. With a one-year appointment to NPS, Dr. Michael will teach the following courses: Introduction to Computer Security, Computing Devices and Systems, Database Security, and Advanced Topics in Computer Security. He will participate in the development of the NPS CISR short course program. His research in the area of policy composition complements that of other NPS CISR researchers and adds a new dimension to the overall program.

NPS CISR will be honored to host Clark Weissman as a visiting professor for one quarter in the fall of 1998. Mr. Weissman has over 35 years of experience in the development of secure systems. His management of secure systems developments have included: models, requirements, architecture, design, specifications, development, testing and assurance evidence generation. Preparations for Mr. Weissman's stay at NPS began at the start of FY98.

2.5 Invited Lecture Series

Leading experts in the field of computer science and INFOSEC from government, academe, and industry are invited to address the students, staff, and faculty at NPS on a regular basis. The lecture series is coordinated with the Department of Computer Science and, when possible, is implemented to extend or enhance NPS CISR courses.

When appropriate, invited lectures are video tapped. In September 1997 techniques to digitize video tapes in order to create CDs of the lectures using web-based techniques were developed.

Presented and planned invited lectures for the period beginning on 1 October 1997 and ending 30 September 1998 are:

- Achieving a Public Key Infrastructure for the U.S. Navy, LCDR Mark Rohrbach SPAWAR, PMW 16, 2 April 1998
- Sun Tzu in Cyberspace, Dr. Thomas A. Berson, Anagram Laboratories, 9 April 1998
- A Unified Framework for Enforcing Multiple Access Control Policies, Pierangela Samarati, SRI International, 10 June 1998
- Klayton Monroe, Arca Systems, NT (In)Security: Data Driven Attacks and Forensics, 20 July 1998.

- Marvin Schaefer, Arca Systems, The Multilevel Policy Model for the Trusted ONTOS Prototype, 22 July 1998.
- William Shockley, Cyberscape, An Axiomatic Specification of Mandatory Security Policies, 29 July 1998.
- Edgar Sibley, George Mason University, The Role of Policy and Law in the Development and Use of Large-Scale Information Systems, 3 August 1998.
- Clark Weissman, Clark Weissman Consulting Co., Network State Synchrony, A Vulnerable Myth,August 10, 1998.
- John McHugh, Portland State University, Policy Considerations for Mobile Nodes, 19 August 1998.
- Lt. Col. Karen Burke, USAFR, Defense Intelligence Agency, Current issues in certification and accreditation of DoD Systems, September 9, 1998.
- Stanley Choffrey, GSA, Government PKI Initiatives, October 16, 1998.

Invited lectures for the period beginning on 1 October 1995 and ending 31 December 1997 were:

- Information Security is Information Security, Ira Winkler, Argo Productions, 21 August 1997.
- CORBA Security and the Sigma Project, Terry C. Vickers-Benzel, Trusted Information Systems, June 1997.
- The IBM SKR Key Recovery System, Dr. Paul A. Karger, IBM T.J. Watson Research Center, 8 May 1997.
- The Secure Composition Problem, Dr. Sylvan Pinsky, National Security Agency, 1 May 1997.
- Multilevel Security - The Neglected Area of Computer Science, James P. Anderson, James P. Anderson, Co., 17 April 1997.
- A System-Oriented Perspective of Computer-Related Risk, Dr. Peter G. Neumann, Computer Science Laboratory, SRI International, 3 April 1997.

Figure 3. An Invited Lecture Series enriches the NPS CISR program. Video taping supports lecture reuse and export. Here Marv Schaefer discusses the challenges of developing a secure Object Oriented Database.

- The Internet Rules but the Emperor Has No Clothes, Dr. Roger R. Schell, Senior Development Manager Information Security, Novell, January 1997.
- Network Security: Threats and Solutions, Dr. Paul A. Karger, Global Security Analysis, January 1997.
- Laboratory, IBM Watson Research Center Modern Identification Models, William R. Shockley, Cyberscape
- Information System Security and Defensive Information Warfare, by Dr. Ron Ross, Institute for Defense Analyses
- An Unusual B3-Compliant Discretionary Access Control Policy, by Jeremy Epstein, Cordant
- Run-Time Security Evaluation for Distributed Applications, by Christina Serban, University of Missouri, Rolla

2.6 Academic Outreach

For the past two years, NPS CISR has hosted the Workshop on Education in Computer Security (WECS). This effort is intended to support the technology transfer efforts of NPS CISR. It brings together both seasoned and new INFOSEC educators and provides them with a venue to share course material, experiences and strategies for effective INFOSEC education. All WECS workshops have been international in scope, with educators from Great Britain, Mexico, Canada, Germany, Belgium, Sweden, and the United States.

The first WECS, held in January 1997, permitted educators to establish a foundation for discussion of computer security education.

Figure 4. The NPS CISR sponsored Second Workshop on Education in Computer Security brought INFOSEC educators together to attend tutorials and share laboratory exercise material. Some of the attendees pose for a snapshot.

In January 1998, the second WECS workshop was held at Asilomar Conference Center in Pacific Grove, CA. The topic of the workshop was the use of laboratory exercises to supplement and enforce concepts taught in the classroom. Each participant submitted a laboratory exercise to share. Prior to the workshop the exercises were bound into a notebook for participants to share. During the workshop each educator had an opportunity to present the exercise and discuss its effectiveness as a teaching tool.

A second benefit of the workshop for attendees was a tutorial on Penetration Testing using the Flaw Hypothesis Methodology by Daniel Faigin, of the Aerospace Corporation. This half day presentation was given by one of the most skilled practitioners of Penetration Testing of Trusted Systems in the security field. It included extensive slides as well as papers for each attendee to take back to their own institutions for incorporation in their own security courses.

Prof. Irvine was a member of the Program Committee for the Second National Colloquium for Information System Security Education. She organized a panel session entitled: Meeting Security Requirements for Global Commerce: Can Education Help? In addition she moderated a working group session addressing the ways that industry can help achieve educational objectives in INFOSEC education. She is on the executive committee for the Colloquium in FY99.

To leverage the benefits of the INFOSEC courses and supplemental materials being developed at NPS, the results of this effort will be made available to other educational institutions. These include the newly emerging program at the University of Maryland as well as those of other colleges and universities.

A web page for NPS CISR has been constructed. The CISR home page provides descriptions of various aspects of the program. It is anticipated that as Web technology advances, materials developed at NPS will be modified to enhance their usability in this new communications paradigm.

It is hoped that the initial prototype effort developed at NPS, targeted primarily at

mid-grade, military officers at the postgraduate level of study, can be expanded to include both undergraduate students at the Service Academies and senior military officers at the National Defense Universities and Senior Service Colleges. The emerging NPS INFOSEC curriculum can be tailored to any of the participating DoD universities and possibly included in the course of study offered by DoD schools servicing the non-commissioned officer corps.

2.7 Graduate Utilization

The immediate placement of NPS CISR graduates in tours of duty that directly utilize their education and expertise continues to be one of NPS CISR's greatest challenges. Advancement in the services often requires officers to command troops or "go to sea." Remarkably, despite the fact that graduates' assignments may not be directly security-related, faculty members have heard from many graduates who both comment on the benefits of their computer security education at NPS and contribute to the prevention of serious security mistakes in system design, configuration, or operation in the fleet.

A number of NPS graduates who conducted thesis research with NPS CISR faculty are currently working in security-related positions. They are:

- Daniel Currie (USN), Fleet Information Warfare Center, Norfolk, VA.
- Julie Lucas (USN), Fleet Information Warfare Center, Norfolk, VA.
- Roy Virden (USN), SNIP Program at NSA, Ft. Meade, MD.
- James Downey (USN), MLS Branch Chief, DISA
- Dion Robb (USN), SPAWARSYSCEN, Charleston, SC.
- Steven Weldon (USN), NAVSECGRU, Ft. Meade, MD
- Bart Umentum (USN), NAVSECGRU, Ft. Meade, MD
- Roger Wright (USA), National Security Agency, Ft. Meade, MD.
- J.D. Fulp (USMC), Instructor, U.S. Naval Academy, Annapolis, MD

A long-term objective of NPS CISR is the placement of graduates in INFOSEC-related positions. With the combined preparation provided through a broad course of study enhanced by a special emphasis on computer security and focused research on a pertinent topic in computer security, NPS CISR graduates are uniquely qualified to participate in DoD computer security research, development, and operational programs. As the importance of computer and network security becomes more evident to the Services, NPS CISR graduates will be prepared to assume leadership positions requiring specialized knowledge of INFOSEC technologies and the systems employing those technologies. Ultimately military speciality codes may be developed to identify this highly trained and educated corps of INFOSEC officers.

2.8 Research

A major objective of this program is to more firmly establish ongoing research in computer security at the Naval Postgraduate School. The benefits of research are many:

- Topics of particular interest to DoD and DoN can be studied at NPS.
- Collaborations on INFOSEC research topics can be established between members of the Computer Science Department and other departments at the Naval Postgraduate School as well as with other security researchers within academe and industry.
- An active faculty research program attracts superior students to participate in the computer security courses and

select security-related topics for thesis work. Student involvement in research has a synergistic effect on faculty research as students combine their operational experience as officers with the expertise provided by faculty members.

DoD has long been involved in the development of secure systems and NPS was active in computer security research as early as 1978, well before the topic became highly visible.The rapid evolution of networking within DoD and DoN has lead to the connection of most computer systems to LANs and the use of WANs for data transport. Security mechanisms have lagged efforts at interconnection and now leave these systems vulnerable to exploitation by adversaries attempting either to compromise information within the systems or deny access to the systems themselves. Security for systems that must process both classified and unclassified information is an underlying theme of the diverse NPS CISR research.

Students from many NPS curricula including: Information Technology Management, C4I, and Information Warfare, join those in Computer Science to conduct thesis research with NPS CISR faculty. Research has included the following information assurance and computer and network security topics: protocols and mechanisms to improve the security of Internet Protocol (IP) over Asynchronous Transfer Mode (ATM) networks; utilization of system mechanisms to provide security for applications in heterogeneous distributed environments; issues associated with security and quality of service; examination of signature identification mechanisms for malicious software, such as viruses; network intrusion detection and response; high assurance techniques for the creation of execution domains; utilization of existing high assurance multilevel products in near-term architectures to achieve operational multilevel secure (MLS) network solutions; product analysis; and innovative approaches to DoD/DoN Networking security problems.

Multilevel Security

A problem for DoD systems includes not only the provision of control of access to and movement of data based on fixed sensitivity levels, but the preservation of compatibility with commercial-off-the-shelf (COTS) application software as well. When compatibility with COTS applications takes precedence, often each access class is relegated to an independent system-high enclave and sharing is achieved through: manual, “sneaker-net” techniques; automated guards for which no notion of sufficiency or completeness with respect to security policy enforcement can be demonstrated; or replication systems relying on physical separation. All can be costly in terms of space, equipment and administration. NPS CISR faculty, staff, and students are constructing a COTS-driven Local Area Network that will provide multilevel secure (MLS) services to users while permitting them to employ standard office productivity tools on standard workstations. The ongoing development centers on the provision of multilevel mail and messaging to the desktop.

Student thesis research centers on the following topics: design of the PC-based TCB extension, protocols for trusted session negotiation on a LAN, trusted accountability mechanisms for the LAN, control of the COTS PC from the TCB extension, and structuring the server application for the multilevel environment. LTs Balmer, Bryer-Joyner, Heller (USN), MAJ Eads (USMC), and CPT Hackerson (USMC) are participating in this effort.

ATM Security

Increasingly, ATM is being used in DoN networks and techniques to move IP traffic over ATM networks are being explored. Unfortu-

nately, current proposed standards for the transport of IP packets over ATM networks are silent regarding packet security. Faculty and students are examining techniques to provide security for IP traffic in ATM networks. Two areas are being investigated: the design of a network access controller to support IP over ATM seamlessly while preventing the flow of unauthorized information from a secure enclave; and investigation of a security protocol and mechanism for fast IP packet forwarding at the data link layer. LT Kondoulis (Hellenic Navy) and CDR Darroca are working in this area.

Intrusion Detection

Defense in Depth, the DoN approach to network security, will use network intrusion detection tools. LT Barrus explored the concept of an intrusion detection system based upon the use of autonomous agents. Deployable in heterogeneous environments, agents would be configurable to their execution environment.

Security for Heterogeneous Systems

The development of systems able to maximize the throughput of jobs across networks of heterogeneous platforms is of great interest to DoD. Factors that must be addressed include communications bandwidth, fault tolerance, and job priorities. Resource management systems are designed to dynamically insure high performance of computationally intensive tasks across multiple networked processors. The evolution of these systems to support adaptable computing in a heterogeneous environment is a topic of research at NPS. To be useful to DoD, these systems must be able to enforce a security policy.

Participating in a project that has as a goal quality of service for end-to-end applications in a highly dynamic environment, NPS CISR faculty, staff, and students are examining techniques to provide security for core services as well as for applications. CPT Wright (USA) developed a layered application architecture that builds upon notions of least privilege and separation of duty. As part of this work, he implemented a demonstration of the architecture using a version of the Intel Common Data Security Architecture (CDSA). A second aspect of this work is to treat processing for security as a factor in overall quality of service delivered by the system. This work will help to parameterize security choices.

Secure Tasking

LT Isa is investigating the hardware and software requirements to support multilevel secure tasking. This research will draw upon fundamental design concepts for security kernels, but will take an innovative approach to the utilization of hardware support.

Load Balancing Firewall

DoN has selected a particular firewall product as one of the components used to protect its networks. As currently deployed, a group of these firewalls is used to protect a given domain. Each firewall is configured for a particular protocol. This configuration leads to under utilization of some of the components and over taxing of others. LT Joyner is working on the design of techniques to distribute work more evenly across the firewalls.

Security for SBU Information

At the request of a SPAWAR PMW 161, LTs Buettner and Harris completed an examination of options for the use of commercial-off-the-shelf (COTS) cryptography to transmit sensitive but unclassified (SBU) data between Navy support installations across the Internet. The students developed a methodology for assessing a variety of encryption products and conducted evaluations on both

Windows 95 and, in some cases, Windows NT. Their work was briefed to VADM Arthur Cerbrowski, N6 at his offices in Washington, D.C. During a tour of the NPS CISR laboratory, Dr. Marvin Langston, then Navy CIO and currently Director, ISO/DARPA, requested a copy of the thesis for review. Their work was completed in September 1997.

JMCIS-Ashore and Java

Currently, JMCIS-Ashore Command and Control System applications are loaded onto each client workstation as a single monolithic application capable of following any of dozens of conditional execution paths. It is often the case that at a given client, a major portion of this software will never be executed. To reduce the amount of software that must be installed, a new paradigm being explored is the use of Java so that machine-independent methods can be dynamically downloaded as execution proceeds. A major benefit of this approach is the ability to rapidly disseminate software updates. Potential dangers include the corruption of data and software either by malicious software downloaded to the clients or servers or by interception and compromise or modification of information along communications paths. LT Weldon has developed a protocol for the authentication of web-based software for use on remote servers.

Security Planning for Wireless Networks

Commercial systems are being deployed which will permit the use of wireless communications for personal and commercial use on a global scale. Assuming that the DoN trend in the use of COTS products continues, it is expected that these satellite systems will be an attractive alternative to land-based communications. LT Fowler is examining the security implications of the use of this technology by DoN.

Secure Web Software

Prof. Volpano, in collaboration with Dr. G. Smith, are exploring how access control requirements could be incorporated into system designed to support remote execution. A concern is to ensure that a remote server's security is not compromised by executing transmitted procedures containing inadvertent or malicious code. Applications must be constrained to prevent the corruption or exfiltration of sensitive information. This research is intended to identify the appropriate security properties of programming languages and to prove that all well-formed programs have them.

A type system for statically checking programs in a basic imperative programming language for illegal information flow has been developed.

Past Efforts

Past research efforts have explored

- The effectiveness of steganography on imagery processed using a lossy compression algorithm such as JPEG,
- Organizational security policies,
- Security in systems intended to host agent software, in particular, the General Magic Telescript system, and
- Analysis of a sanitization system being deployed by DoN.

Student Research Travel

Through travel funds support, NPS CISR has been able to send students to conferences and meetings pertinent to their thesis research. Supported through curriculum funds, two Information Warfare students, LTs Buettner and Harris spent a six week experience tour during the winter quarter of FY97 working for Dr. Carl Landwehr at the Naval Research Laboratory in Washington, D.C.

LTs Downey, Robb and English attended the IEEE Symposium on Security and Privacy in May 1997. At this conference LT Downey along with NPS Visiting Professor William Shockley comprised a debate team arguing the negative response to the following question: "Is the Trusted Computing Base Concept Fundamentally Flawed?" Their opponents were Bob Blakley, of IBM, and Darrell Kienzle, of the Univ. of Virginia, who unsuccessfully defended William Wulf's premise that the notion of the TCB was flawed and inadequate to describe modern systems.

MAJ Eads and LT Isa attended the National Information Systems Security Conference in Baltimore, Maryland in October 1997. CPT Hackerson attended the Computer Security Applications Conference in December 1997. The 1998 IEEE Symposium on Security and Privacy was attended by LTs Bryer-Joyner, Isa, Heller, MAJ Eads, and CPT Hackerson. LTs Bryer-Joyner and Joyner spent a week at SPAWARSYSCEN, Charleston, SC to conduct thesis research and investigate collaborative programs between that organization and NPS CISR.

3. NPS CISR Awards

The efforts of NPS CISR faculty and staff are being recognized both at NPS and beyond.

- Naval Postgraduate School award for Outstanding Research Achievement, Information Warfare Academic Group, 1997, to Professor. Irvine, awarded in May 1998.
- Naval Postgraduate School award for Outstanding Research Achievement, Computer Science Department, 1996, to Professor. Volpano, awarded in May 1997.
- ACM Service Award, Workshop on Education in Computer Security, 1997, to Professor Irvine.

4. Future Plans

Future plans at NPS CISR include both the continued enhancement of the CISR's instructional capabilities and its many INFOSEC research projects. Both long- and short-term efforts have been launched and most of these projects are, to some extent, funded. We hope to advance these projects from prototypes to completion. In addition, we will work with DoN/DoD and U.S Government to identify extensions to our work that will address new INFOSEC concerns.

4.1 Curriculum Development

In the first quarter of FY99, NPS CISR will host Clark Weissman as a visiting professor. He will teach secure systems from the perspective of a penetration analysis using the Flaw Hypothesis Methodology. The target of evaluation will be Windows NT. We plan to video tape the entire class.

In other areas, we will continue development of the database security course, that had its initial offering in the Spring Quarter of FY98. This will be facilitated by our other visiting professor, Dr. Michael, whose doctoral studies involved extensive scrutiny of security issues associated with database management systems.

We plan to continue development of other courses to ensure that they provide both the technical foundations required for a firm grounding in computer science as well as incorporation of state of the art advances in theory, practice and technology. Several of our courses are well developed, however others have been taught only a few times and require continued effort.

We are planning to adapt Introduction to Computer Security so that it can be presented as a short course. The motivation for this has come from requests by DoD organiza-

tions for a computer security course that will satisfy specific requirements.

4.2 Computer Security Laboratory

To support the class on secure systems through a penetration analysis of Windows NT, several additional NT platforms will be acquired. We plan to assign five students per platform. Enrollment in the class is restricted to 25 participants.

The access control features of Windows NT will be used to illustrate a number of concepts taught in Introduction to Computer Security. Plans are being made to convert a number of the laboratory exercises to the Windows NT format.

We wish to develop a laboratory capability for the students to be able to assemble physical networks for various security experiments. These components will include both software and hardware:

- Firewalls
- Encryption toolkits
- Commercial versions of network authentication or token mechanisms
- Boundary controllers
- Routers
- Hubs
- Hardware and software VPN components

4.3 Faculty Development

The faculty development program will be used to assist appropriate members of the Computer Science, Electrical and Computer Engineering, and Mathematics Departments expand their understanding of INFOSEC.

4.4 Visiting Professor Program

During FY99, NPS CISR will host Clark Weissman as a Visiting Professor for the Fall Quarter. Dr. Bret Michael will continue his one year appointment as a Visiting Associate Professor. As the year progresses, plans will be made to identify a distinguished visiting professor for FY00.

4.5 Invited Lecture Series

The invited lecture series will be continued throughout the coming year. The use of the course entitled Advanced Topics in Computer Security as a context for the invited lecture series will be continued. Through the continued cooperation of the Computer Science Department's Modeling and Visual Simulation Curriculum, NPS CISR will be able to leverage the most advanced technologies in video recording and display to capture lectures for future incorporation in instructional materials.

4.6 Academic Outreach

NPS CISR faculty will continue to foster INFOSEC education through a variety of programs.

In January 1998 NPS will be host to the third Workshop on Education in Computer Security.

NPS CISR will continue to support the NSA-sponsored intensive faculty development program in the late summer to early fall time frame.

Information and materials developed by NPS for the CISR curriculum will be made available to other educational institutions. The NPS CISR Web Server will continue to permit the dissemination of materials far beyond the confines of DoD. It can make the NPS CISR INFOSEC curriculum and supporting course materials available to a potentially very large number of users. NPS CISR faculty are continuing to explore both synchronous and asynchronous distance learning.

Dr. Irvine is a member of the Executive

Committee of the National Colloquium for Information Systems Security Education, which will take place in May 1999. She is also a member of the Program Committee of the First World Conference on Computer Security Education, sponsored by IFIP, which will be held in Stockholm, Sweden in June 1999.

Given sufficient funding, NPS CISR wishes to support outreach chairs in INFOSEC. The intent would be to allow university professors with no background in INFOSEC to participate in NPS CISR programs for six months to a year. These professors would be given temporary positions in the Computer Science Department at NPS. During that time they will teach computer science classes, conduct basic research, and assist students with thesis work. Upon completion of the appointment, the visiting professors would return to their respective academic institutions with a comprehensive INFOSEC curriculum plan and a set of supporting curriculum course materials.

4.7 Graduate Utilization

NPS CISR students and faculty will continue to explore ways in which the advanced education in INFOSEC of graduates can be leveraged by DoD/DoN and government.

4.8 Research

Several research programs have been launched with the support of NPS CISR. Several have successfully established independent funding bases. As the faculty and staff of the program has grown, the benefits of "critical mass" in terms of research activity are becoming evident.

The NPS CISR research program is thriving. It is anticipated that the productivity of the faculty, staff and students will increase. Areas of research are broad and include: multilevel security, network security, policy composition, language theory as applied to security, database security, and applications security.

5. Conclusion

NPS CISR is becoming a world class center for computer and information system security education and research. The expertise and commitment of its faculty and staff combined with the raw talent and energy of its students is already providing DoD with an unparalleled, multifaceted program. The course of study provides students with a firm grounding in the foundations of computer science and conveys vital concepts and techniques associated with INFOSEC today. Our research programs are varied and address DoD/DoN concerns. A new generation of officers able to address the challenges in computer security and information assurance that lie ahead is being created.

Acknowledgments

We gratefully acknowledge the support and encouragement of the sponsors of our research including the National Security Agency, DISA, SPAWAR, National Imagery and Mapping Agency, DARPA/ITO, DARPA/ISO, and Naval Postgraduate School Direct Funding Program.

Members of NPS CISR

- Cynthia E. Irvine, Assistant Professor of Computer Science, Director NPS CISR.
- Hal Fredericksen, Professor of Mathematics.
- Gilbert Lundy, Associate Professor of Computer Science.
- J. Bret Michael, Visiting Associate Professor of Computer Science.
- Neil C. Rowe, Associate Professor of Computer Science.
- Timothy Shimeall, Associate Professor of

Computer Science.

- Dennis Volpano, Assistant Professor of Computer Science
- Daniel Warren, Adjunct Professor of Computer Science.
- Geoffrey Xie, Assistant Professor of Computer Science.
- Paul Clark, Laboratory Manager and Research Staff, NPS CISR.
- Anastacia Cruz-Tokar, Laboratory Assistant, NPS CISR.
- Timothy Levin, Senior Research Associate, NPS CISR.
- Richard Saunders, Analyst, NPS CISR

Appendix A: NPS CISR Courses

Current courses in the NPS CISR program are described below and are integrated into the Computer Science curriculum as illustrated in Table 1.

Introduction to Computer Security

This course is concerned with fundamental principles of computer and communications security for modern monolithic and distributed systems. It covers privacy concerns, data secrecy and integrity issues, as well as DoD security policy. Security mechanisms introduced will include access mediation, cryptography, authentication protocols, and multilevel secure systems. Students will be introduced to a broad range of security concerns including both environmental as well as computational security. Laboratory facilities will be used to introduce students to a variety of security-related technologies including, discretionary access controls in Class C2 systems, mandatory access controls in both low and high assurance systems, identification and authentication protocols, the use of cryptography in distributed systems, and database technology in trusted systems.

Secure Management of Secure Systems

This course is intended to provide students with an understanding of management concerns associated with computer-based information systems. Students will examine the security concerns associated with managing a computer facility. The impact of configuration management on system security, the introduction of software that must be trusted with respect to computer policies, environmental considerations, and the problems associated with transitions to new systems and technology will be studied in the context of Federal Government and especially DoD information systems.

Network Security

This course presents topics in network security for both open systems and military/intelligence networks. Network security is needed for applications ranging from the transmission of simple messages to electronic commerce to the secure execution of remote, and sometimes, mobile code. Students will review the cryptography commonly employed in networked systems and the strengths and weaknesses of several cryptographic protocols. Approaches to key management in small and large scale enterprises will be explored. Current issues including the interaction of multiple security policies, the binding of cryptographic authentication to access control, and integrity in both open and military systems will be addressed. Case studies will allow students to understand the complexity of applying cryptography to real systems.

Secure Systems

This course covers implementation of protection domains for both monolithic and distributed secure systems. The importance of system architecture to assurance methodologies for security kernels will be emphasized. Topics will include the use of protection hardware, the implementation of virtual machines through the effective use of memory management techniques including segmentation and paging, synchronization mechanisms, critical sections, software engineering methodologies as applied to the development of secure systems, and configuration management techniques.

Database Security

This course covers the logical issues associated with database security. Policies for integrity and confidentiality of information will be reviewed in the context of database systems. Modeling of secure database systems will be covered along with implemen-

Table 1. Computer Security Track

1st Quarter (Fall or Spring)	CS2971 (3-2) Object-Oriented Programming in C++, Part I	CS-3010 (4-0) Computing Devices and Systems	MA3025 (5-1) Logic and Discrete Mathematics	MA3030 (5-1) Intro. to Combinatorics & Its Applications	
2nd Quarter (Winter or Summer)	CS3971 (3-2) Object-Oriented Programming, in C++, Part II	CS3300 (3-2) Data Structures	CS3200 (3-2) Introduction to Computer Architecture	CS3601 (4-0) Theory of Formal Languages & Automata	CS4900 (2-0) Research Seminar in Computer Science
3rd Quarter (Spring or Fall)	CS377x (3-2) Object-Oriented Programming (Ada or Java)	CS3310 (4-0) Artificial Intelligence	CS3600 (3-2) Introduction to Computer Security	CS3460 (3-1) Software Methodology	CS4900 (2-0) Research Seminar in Computer Science
4th Quarter (Summer or Winter)	CS3650 (4-0) Theory of Algorithms	CS3320 (3-1) Database Systems	CS3450 (3-2) Operating Systems	CS3111 (4-0) Principles of Programming Languages	
5th Quarter (Fall or Spring)	CS3502 (4-0) Computer and Communica-tions Networks	CS3670 (3-2) Secure Management of Systems	CS4600 (3-2) Secure Systems	Track Requirement	
6th Quarter (Winter or Summer)	CS4203 (3- Interactive Computation Systems	Thesis	CS4112 (3-2) Distributed Operating Systems	CS4605 (3-1) Security Policies, Models and Formal Methods	
7th Quarter (Spring or Fall)	NS3252 (4-0) Joint & Mari-time Strategic Planning	Thesis	CS4603 (3-2) Database Security	Track Requirement	Note: International students replace NS-3252 with IT-1500.
8th Quarter (Summer or Winter)	Thesis	Thesis	CS3690 (4-0) Network Security	CS4614 (3-1) Advanced Topics in Computer Security	

Bold Outline indicates courses specifically required for the Computer Security Track

The track requirements in the 5th and 7th quarters are determined as appropriate based on the thesis research and interests of the individual student. and include options for Introduction to Compiler Writing, Computability Theory and Complexity, Advanced Object Oriented Program with JAVA, Cryptography and other courses as needed.

tation issues including atomicity, serialization, and view-based control. Releasability issues in secure database design will be addressed. Security in statistical databases will be addressed along with security approaches for object oriented databases. Novel approaches to the collection and use of audit databases will be addressed including intrusion detection.

Security Policies, Models, and Formal Methods

The course covers the methods used to specify, model, and verify computational systems providing access control. The identification of the security policy and its interpretation in terms of a technical policy for automated systems is covered. Informal and formal security policy models are discussed and several access-control models are explored including information-flow models, the Access Matrix Model, the Bell and LaPadula Model, nondeducibility, and noninterference. Policy expressed in terms of the entities on a computer is reviewed. Formal models and proof of their correctness provide the bridge between a written statement of security policy and the implementation of a particular secure system. Topics include access control, information flow, safety, and verification. Verification methods are discussed.

Advanced Topics in Computer Security

This course covers advanced topics in software, communications and data security. Military and commercial information security and integrity policies will be studied. Software and hardware subversion of computer systems; advances in operating system, database, and network security, evaluation criteria for secure systems, modal logic and linear and branching-time temporal logics, cryptographic and authentication protocols, and techniques for implementing supporting policies.

Appendix B: Publications

This section lists publications by NPS CISR faculty, staff and students.

Papers

[1] Wright, R.E., Sheffield, D.J., and Irvine, C. E., "Security for a Virtual Heterogeneous Machine," to appear in the *Proceedings of the Twelfth Computer Security Applications Conference*, Scottsdale, AZ, December 1998.

[2] Confinement Properties for Programming Languages, Dennis Volpano and Geoffrey Smith, To appear in SIGACT News, 1998.

[3] Irvine, C.E., Anderson, J.P., Robb, D.A., and Hackerson, J.,"High Assurance Multilevel Services for Off-The-Shelf Workstation Applications," to appear in *Proceedings of the National Information Systems Security Conference*, October 1998.

[4] Barrus, J. and Rowe, N.C., "A Distributed Autonomous-Agent Network-Intrusion Detection and Response System," *Procedings of the 1998 Command and Control Research and Technology Symposium*, Monterey CA, June-July 1998.

[5] Volpano, D. and Smith, G., "Probabilistic Noninterference in a Concurrent Language," *Proc. 11th IEEE Computer Security Foundations Workshop*, pp. 34-43, Rockport, MA, June 1998.

[6] Volpano, D. and Smith, G., "Language Issues in Mobile Program Security," In Mobile Agents and Security, G. Vigna (Ed.), volume 1419 of Lecture Notes in Computer Science, pp. 25-43. Springer Verlag, 1998.

[7] Smith, G. and Volpano, D., "Secure Information Flow in a Multi-threaded Imperative Language," *Proc. 25th ACM Symposium on Principles of Programming Languages*, pp.355-364, San Diego, CA, January 1998.

[8] Irvine, C.E., "Naval Postgraduate School Center for INFOSEC Studies and Research: Teaching the Science of Computer Security," *MILCOM Proceedings (classified)*, Monterey, CA, November 1997.

[9] Irvine, C.E., Warren, D.F., and Clark, P.C., "The NPS CISR Graduate Program in INFOSEC: Six Years of Experience," *Proceedings of the 20th National Information Systems Security Conference*, Baltimore, MD, pp 22-30, October 1997.

[10] Irvine, C.E., "Computer Security Education Challenges," *IEEE Software*, Vol. 14, No. 5, September 1997, pp 110-111.

[11] Volpano, D., and Irvine, C.E., "Secure Flow Typing," *Computers and Security*, Vol 16, No.2, 1997, pp 137-144.

[12] Irvine, C.E., "The First ACM Workshop on Education Computer Security," *ACM SIGSAC Review*, Vol 15, No. 2, pp 3-5, 1997.

[13] Irvine, C.E., "Security in Innovative New Operating Systems," *Proceedings IEEE Symposium on Security and Privacy*, May 1997, pp. 202-203.

[14] Volpano, Dennis, Smith, Goeff and Irvine, Cynthia, "A Sound Type System for Secure Flow Analysis," *Journal of Computer Security*, Vol 4, No. 3, 1996, pp 1-21.

[15] Currie, D. L, and Irvine, Cynthia E., "Surmounting the Effects of Lossy Compression in Steganography," *Proceeding of the 19th Information Systems Security Conference*, Baltimore, Maryland, October 1996, pp 194-201.

[16] Volpano, D. and Smith, G., "On the Systematic Design of Web Languages," ACM Computing Surveys, Vol. 28, No. 2, pp. 315-317, June 1996.

[17] Irvine, Cynthia E., Goals for Computer Security Eduation, *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California, May 1996, pp 24-25.

[18] Irvine, Cynthia E., A Multilevel File System for High Assurance, *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California, May 1995, pp 78-87.

Technical Reports

[1] Irvine, C.E. and Shockley, W.R., *Roundhouse: A Security Architecture for Active Networks*, Naval Postgraduate School Technical Report, NPSCS-98-002, Naval Postgraduate School, Monterey, CA, May 1998.

[2] Chin, S-K, Irvine, C.E., and Frinke, D., *An Information Security Education Initiative for Engineering and Computer Science*, Naval Postgraduate School Technical Report, NPSCS-97-003, Naval Postgraduate School, Monterey, CA, December 1997.

[3] Irvine, C.E., Warren, D. F., and Stemp, R., *Teaching Computer Security at a Department of Defense University*, NPS-CS-97-002, April 1997.

Web-Based Publications

[1] Irvine, C.E., "Workshop on Education in Computer Security (WECS '98)", *Electronic Cipher* #3, April. 27, 1998, IEEE Computer Society TC on Secu-

rity and Privacy.
URL http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/

[2] Irvine, C.E., "Report on the Defensive Information Warfare Symposium", *Electronic Cipher* #3, Dec. 23, 1995, IEEE Computer Society TC on Security and Privacy.
URL http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-archive.html

[3] Irvine, C. E, "Report on Tenth Annual Computer Security Applications Conference," *Electronic Cipher* #3, Jan. 13, 1995, IEEE Computer Society TC on Security and Privacy.
URL: http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-archive.html

Presentations: Conference, Workshop, and Invited Talks

[1] Irvine, C.E., *Meeting Security Requirements for Global Commerce: Can Education Help?*, (Panel organization and presentation), National Colloquium for Information Systems Security Educaiton,, Harrisonburg VA, June 1998.

[2] Irvine, C.E., *Enforcement of Security Policies*, A.C.M. Invited talk, Bowling Green State University, Bowling Green, OH, March 1998.

[3] Warren, D.F.,"Virus Lab," Workshop on Education in Computer Security, Pacific Grove, CA, January 1998.

[4] Irvine, C.E., "Exploitation of a Covert Channel," Workshop on Education in Computer Security, Pacific Grove, CA, January 1998.

[5] Irvine, C.E., "Naval Postgraduate School Center for INFOSEC Studies and Research: Teaching the Science of Computer Security," MILCOM, Monterey, CA, November 1997.

[6] Irvine, C. E., Warren, D. F., and Stemp. R., "The NPS CISR Graduate Program in INFOSEC: Six Years of Experience," 20th National Information Systems Security Conference, Baltimore, MD, October 1997.

[7] Irvine, C.E., "Teaching Introduction to Computer Security", presented at the NSA Workshop on Teaching INFOSEC, Monterey, CA, September 1997.

[8] Irvine, C.E., "Graduate Education in Computer Security", National Colloquium for Information Systems Security Education, Baltimore, MD, April 1997. Invited speaker.

[9] Irvine, C. E., "University Education in Computer Security," *Federal Information System Security Education Association*, Gaithersburg, MD, March 1997. Invited speaker.

[10] Currie, D. L, and Irvine, Cynthia E., "Surmounting the Effects of Lossy Compression in Steganography," *19th Information Systems Security Conference*, October, 1996.

[11] Volpano, Dennis, "Type Systems for Secure Remote Evaluation," 12th Mathematical Foundations of Programming Semantics, Boulder, CO, June 1996.

[12] Irvine, Cynthia E., "Graduate Education in Computer Security," INFOSEC Research Council meeting, Alexandria, Virginia, August 1996.

[13] Volpano, Dennis, "Provably-Secure Programming Languages for Remote Evaluation," Workshop on Strategic Directions in Computing Research, MIT June 1996.

[14] Irvine, Cynthia E., "Goals for Computer Security Education," *IEEE Symposium on Security and Privacy*, Oakland, May 1996.

Appendix C: NPS CISR Theses

MS Theses

[1] Steven Balmer (USN) , *Trusted Computing Base Extension Control System For Client Workstations*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date September 1999.

[2] Dan Morris (USMC), *VPN Management for the USMC*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date September 1999.

[3] Susan Bryer-Joyner (USN), *Trusted Accountability Mechanism for the XTS-300 Ethernet Port*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date March 1999.

[4] James Fowler (USN), *Security Planning for Wireless Networks*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date March 1999.

[5] Scott D. Heller (USN) , *A Protocol for Establishing a Trusted Path Over an Untrusted Local Area Network*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date March 1999.

[6] Lee Joyner (USN) , *Development of a Load-Balancing Mechanism for Parallel Firewalls*, Masters Thesis, Naval Postgraduate School, Monterey, California,

anticipated graduation date March 1999.

[7] Haruna Isa (USN), *Utilizing Hardware Features for Secure Thread Management*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date December 1998.

[8] Jason Hackerson (USMC), *Constructing a Trusted Computing Base Extension in Commercial-Off-the Shelf Personal Computers for Multilevel Secure Local Area Networks*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date September 1998.

[9] Gregorio G. Darroca (USN), *A Flow-Based Security Protocol for Fast IP Tag Switching*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date September 1998.

[10] Wright, Roger (USA), *Integrity Architecture and Security Services Demonstration for Management System for Heterogeneous Networks*, Masters Thesis, Naval Postgraduate School, Monterey, California, June 1998

[11] William A. Macchione (USN), The Capabilities, Propagation Effects, and Targeting of Computer Systems, Masters Thesis, Naval Postgraduate School, Monterey, California, March 1998.

[12] Joe Barrus, *Intrusion Detection in Real-Time in a Multi-Node Multi_Host Environment*, Masters Thesis, Naval Postgraduate School, Monterey, California, September 1997.

[13] Ray Buettner (USN) and Robert Harris (USN), *Comparative Analysis of Commercial Off The Shelf (COTS) Encryption Products for Use in Transmitting Sensitive But Unclassified (SBU) Data*, Masters Thesis, Naval Postgraduate School, Monterey, California, September 1997.

[14] James Downey (USN) and Dion Robb (USN), *A High Assurance Label-Based Mail Service for LANs*, Masters Thesis, Naval Postgraduate School, Monterey, California, 1997.

[15] John English (USN), *Security Analysis for a Management System for Heterogeneous Networks (MSHN)*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date September 1997.

[16] H. Steve Kremer, *Practical Applications of Real-Time Intrusion Detection in a Multinode Environment*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date September 1997.

[17] Steve Weldon (USN), *Security Issues in the JMCIS-Ashore Command and Control System*, Masters Thesis, Naval Postgraduate School, Monterey, California, anticipated graduation date September 1997.

[18] Bart Umentum (USN), *Using Web Technology to Disseminate INFOSEC Lectures*, Masters Thesis, Naval Postgraduate School, Monterey, California, September 1997.

[19] Lee A. Heaton (USN), *Radiant Mercury: An Assessment of the Issues*, Masters Thesis, Naval Postgraduate School, Monterey, California, September 1996.

[20] Julie Lucas (USN), Ensuring a C2 Level of Trust and Interoperability in a Networked Windows NT Environment, Masters Thesis, Naval Postgraduate School, Monterey, California, September 1996.

[21] Robert Marlett (USN), *Analysis of General Magic Telescript with Respect to Class C2 Requirements*, Masters Thesis, Naval Postgraduate School, Monterey, California, September 1996.

[22] LT Hannelore Campbell (USN) and LT Daniel L. Currie, III (USN), *Implementation and Efficiency of Steganographic Techniques in Bitmapped Images and Embedded Data Survivability Against Lossy Compression Schemes*, Masters Thesis, Naval Postgraduate School, Monterey, California, March 1996.

[23] John D. Fulp (USMC), *A National Imagery System Security Policy*, MastersThesis, Naval Postgraduate School, Monterey, California, March 1996.

[24] David Wootten (USN), *A Graphic User Interface for Rapid Integration of Steganography Software*, Masters Thesis, Naval Postgraduate School, Naval Postgraduate School, Monterey, California, March